(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10214255 A

(43) Date of publication of application: 11 . 08 . 98

(51) Int. Cl G06F 15/00
G06F 12/14

(21) Application number: 09018039

(22) Date of filing: 31 . 01 . 97

(71) Applicant: FUJI XEROX CO LTD

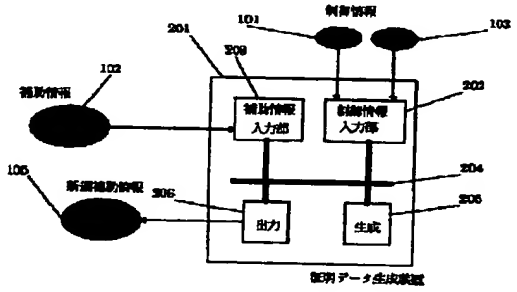
(72) Inventor: CHIBA KENJI
KIYOUJIMA HITOKI

(54) METHOD AND DEVICE FOR GENERATING CERTIFICATION DATA

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a certification data generation technique for changing limit information such as the generation condition of an authority at a user's side.

SOLUTION: Auxiliary information 102 is inputted from an auxiliary information inputting part 203, and control information 101 corresponding to the auxiliary information 102 is inputted to a control information inputting part 202. Moreover, a user inputs new control information to the control information inputting part 202. The inputted control information and auxiliary information is transmitted through a data bus 204 to an auxiliary information generating part 205. The auxiliary information generating part 205 calculates new auxiliary information from the transmitted control information and auxiliary information based on a prescribed expression, and transmits the result through the data bus 204 to an auxiliary information outputting part 206. The auxiliary information outputting part 206 outputs the transmitted new auxiliary information 105.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－214255

(43)公開日　平成10年(1998)８月11日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｚ
	12/14	３１０		12/14	３１０Ｄ

審査請求　未請求　請求項の数13　ＯＬ　（全 13 頁）

(21)出願番号　特願平9－18039

(22)出願日　平成９年(1997)１月31日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　千葉　健司
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　京嶋　仁樹
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

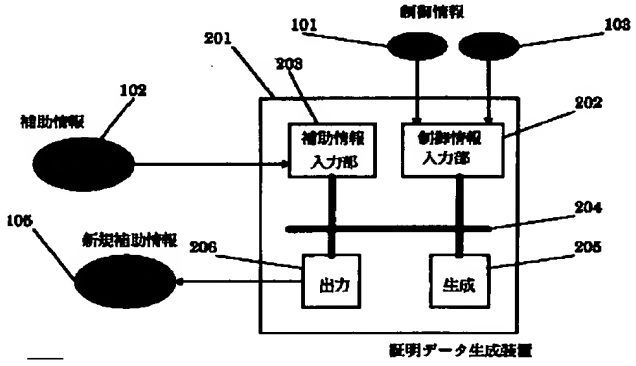
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　証明データ生成方法および装置

(57)【要約】

【課題】　権利の発生条件等の制限情報を使用者側で変更できるようにした証明データ生成技術を提供することを目的としている。

【解決手段】　補助情報１０２を補助情報入力部２０３から入力するとともに、補助情報１０２に対応する制御情報１０１を制御情報入力部２０２に入力する。さらに利用者が新規の制御情報を制御情報入力部２０２に入力する。入力された制御情報および補助情報はデータバス２０４を通じて、補助情報生成部２０５に送られる。補助情報生成部２０５は送られてきた制御情報と補助情報から新規補助情報を、所定の式に基づいて計算し、結果をデータバス２０４を通じて、補助情報出力部２０６に送る。補助情報出力部２０６は送られてきた新規補助情報１０５を出力する。



1

【特許請求の範囲】

【請求項１】　入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成方法において、

新たに設定したい制御情報と、現在の補助情報と、上記現在の補助情報を生成するのに用いた古い制御情報とに基づいて新たな補助情報を生成するステップと、

上記新たな補助情報に基づいて新たな証明データを生成するステップとを有することを特徴とする証明データ生成方法。

【請求項２】　上記補助情報は、上記制御情報と使用者の固有情報とに基づいて生成される請求項１記載の証明データ生成方法。

【請求項３】　上記制御情報は権利の発生条件および証明データを生成するときの副作用を規定する請求項１または２記載の証明データ生成方法。

【請求項４】　既存の制御情報を変更することによりあらたな制御情報を生成する請求項１、２または３記載の証明データ生成方法。

【請求項５】　入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成装置において、

上記制御情報を入力する手段と、

上記補助情報を入力する手段と、

入力された補助情報と、上記補助情報を生成するのに用いた制御情報と、新たに入力された制御情報とに基づいて新たな補助情報を生成する手段と、

上記新たな補助情報に基づいて新たな証明データを生成する手段とを有することを特徴とする証明データ生成装置。

【請求項６】　入力された制御情報を記憶する手段を設けた請求項５記載の証明データ生成装置。

【請求項７】　入力された制御情報と補助情報の正当性を検証する手段を設けた請求項５または６記載の証明データ生成装置。

【請求項８】　入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成装置において、

上記制御情報を記憶する手段と、

現在記憶されている制御情報に対応する補助情報を入力する手段と、

上記現在記憶されている制御情報から新たな制御情報を生成する手段と、

現在記憶されている制御情報と、現在記憶されている制御情報に対応する補助情報と、新たに生成された制御情報とに基づいて新たな補助情報を生成する手段と、

上記新たな補助情報に基づいて新たな証明データを生成する手段とを有することを特徴とする証明データ生成装置。

2

【請求項９】　上記新たに制御情報を生成する手段は、制御情報の生成方法を制御する生成制御情報によって制御情報の生成の仕方を制御する請求項８記載の証明データ生成装置。

【請求項１０】　上記生成制御情報を使用回数の情報とし、使用回数と所定の値とを比較してその結果に応じて上記制御情報を変更する請求項９記載の証明データ生成装置。

【請求項１１】　上記生成制御情報を使用時間の情報とし、使用時間と所定の値とを比較してその結果に応じて上記制御情報を変更する請求項９記載の証明データ生成装置。

【請求項１２】　上記生成制御情報を記憶する手段を設けた請求項９、１０または１１記載の証明データ生成装置。

【請求項１３】　上記生成制御情報を入力する手段を設けた請求項９、１０、１１または１２記載の証明データ生成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、利用者の権利を証明するデータを生成する、証明データ生成方法および装置に関する。

【０００２】

【従来の技術】利用者の権利を制御するような技術としては、例えば特開平４－１５７５５５号公報に記載されているものがある。この技術においては、利用者のＩＤと利用者の権利情報とをホストコンピュータに保持し、端末から入力される利用者のＩＤから利用者の権利情報を検索し、検索の結果得られた権利情報に応じた範囲で利用を許可し、所定のサービス提供の制御を行う。

【０００３】しかし前述の従来の技術においては、利用者の権利を変更するには、ホストコンピュータの情報を書き換えなければならない。したがって、変更作業はホストコンピュータの管理者が行う必要がある。そのため、大量の利用者情報を管理しなければならない場合、利用者情報の管理負荷がホストコンピュータおよびその管理者に集中してしまう。

【０００４】

【発明が解決しようとする課題】本発明は、以上の事情を考慮してなされたものであり、権利の発生条件等の制限情報を使用者側で変更できるようにした証明データ生成技術を提供することを目的としている。

【０００５】

【課題を解決するための手段】本発明においては、入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する構成において、利用者

側に、制御情報と補助情報とを用いて新たな補助情報を生成する手段を設けることで、上記の問題を解決するものである。すなわち、センタ側は利用者の基本的な権利情報（ＩＤなど）のみを保持し、資源への利用権利の変更については、制御情報を利用者に与えるのみにすることができる。場合によっては利用権利の変更方法をあらかじめ利用者にもたせることも可能となるので、センタ側の負荷を低減することができる。

【０００６】すなわち、本発明によれば、上述の目的を達成するために、入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成方法において、新たに設定したい制御情報と、現在の補助情報と、上記現在の補助情報を生成するのに用いた古い制御情報とに基づいて新たな補助情報を生成するステップと、上記新たな補助情報に基づいて新たな証明データを生成するステップとを行うようにしている。

【０００７】この構成においては、利用者側において新たな制御情報を設定するのみで補助情報を変更することができ制御情報を変更する度に保持情報を利用者側に送る必要がなくなる。

【０００８】また、この構成において、上記補助情報は、上記制御情報と使用者の固有情報とに基づいて生成されるようにでき、また、上記制御情報は権利の発生条件および証明データを生成するときの副作用を規定するものとすることができる。

【０００９】副作用としては、証明データの生成（すなわち証明の結果例えばコンテンツを利用することになった場合には、その利用）に対する価格がある。これにより、利用量課金システムを実現できる。また、他の副作用としては例えば補助情報の有効期間がある。これにより、コンテンツ等の利用期間を規定できる。例えば、コンテンツ自体には利用期間を管理する機構を含めることなく、コンテンツの利用時間を補助情報の有効期間により間接的に管理できる。

【００１０】また、既存の制御情報を変更することによりあらたな制御情報を生成するようにしてもよい。

【００１１】また、本発明によれば、上述の目的を達成するために、入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成装置に、上記制御情報を入力する手段と、上記補助情報を入力する手段と、入力された補助情報と、上記補助情報を生成するのに用いた制御情報と、新たに入力された制御情報とに基づいて新たな補助情報を生成する手段と、上記新たな補助情報に基づいて新たな証明データを生成する手段とを設けるようにしている。

【００１２】この構成においても、制御情報を変更する度に保持情報を利用者側に送る必要がなくなる。

【００１３】また、この構成において、入力された制御情報を記憶する手段を設けてもよいし、入力された制御情報と補助情報の正当性を検証する手段を設けてもよい。

【００１４】また、本発明によれば、上述の目的を達成するために、入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成装置に、上記制御情報を記憶する手段と、現在記憶されている制御情報に対応する補助情報を入力する手段と、上記現在記憶されている制御情報から新たな制御情報を生成する手段と、現在記憶されている制御情報と、現在記憶されている制御情報に対応する補助情報と、新たに生成された制御情報とに基づいて新たな補助情報を生成する手段と、上記新たな補助情報に基づいて新たな証明データを生成する手段とを設けるようにしている。

【００１５】この構成においても、制御情報を変更する度に保持情報を利用者側に送る必要がなくなる。

【００１６】また、この構成において、上記新たに制御情報を生成する手段は、制御情報の生成方法を制御する生成制御情報によって制御情報の生成の仕方を制御するようにしてもよく、また、上記生成制御情報を使用回数の情報とし、使用回数と所定の値とを比較してその結果に応じて上記制御情報を変更するようにしてもよい。また、上記生成制御情報を使用時間の情報とし、使用時間と所定の値とを比較してその結果に応じて上記制御情報を変更するようにしてもよい。また、上記生成制御情報を記憶する手段を設けけもよく、上記生成制御情報を入力する手段を設けてもよい。

【００１７】

【発明の実施の形態】

［認証システムの概要］まず、本発明の実施例について説明する前に、本発明の実施例が前提とする認証システムについて説明する。なお、本発明は、以下の認証システム以外にも適用可能である。

【００１８】本発明の実施例が前提とする認証システムには、図１に示すように、３つのエンティティ、すなわち、管理センタ１、プロバイダ２、利用者３が存在する。プロバイダ２は、情報、装置、あるいは資源（以下コンテンツと総称する）をもち、それに対する利用者３のアクセスを制御したい。このような場合、公知の技術である公開鍵暗号技術を用いることができる。以下この公開鍵暗号技術の使用を前提にする。

【００１９】公開鍵暗号技術にしたがって、各エンティティはそれぞれ以下のような情報を持つ。

管理センタ１　：　センタの公開鍵ペア（ｅｃ，ｎｃ）、署名鍵ｄｃ（秘密）

利用者３　：　認証鍵ｄｕ（秘密）

プロバイダ２　：　コンテンツ暗号鍵Ｋ（秘密）

管理センタ１の鍵はたとえばＲＳＡ（Ｒｉｖｅｓｔ、Ｓｈａｍｉｒ、Ａｄｌｅｍａｎ）暗号技術のような公開鍵暗号技術に基づいて作られる。利用者３は、ｄｕを封入したトークンと呼ばれる利用者固有の認証装置（トークン）３１と、コンテンツを利用するためのコンテンツ利用プログラム３２とを持つ。基本的に利用者３はあるコンテンツに対してアクセスするため、アクセス制御を行う情報（以下チケットと呼ぶ）をセンタ１に発行してもらう。利用者はこのチケットと、トークンと呼ばれる利用者固有の認証装置３１を用いて、資源へのアクセスが可能となる。

【００２０】このチケット発行の準備として、以下のことが行われる。

【００２１】まず、プロバイダ２は管理センタ１に依頼して、特定の資源に対する情報ｎ（以下これをチケット法数と呼ぶ）とＥ（チケット公開鍵と呼ぶ）を生成してもらう。ｎは、暗号学的に安全な２つの素数ｐ，ｑを用いて、ｎ＝ｐ・ｑとして、生成する。ｎには、管理センタ１の電子署名が施される。さらに管理センタ１はＥとｎを保持する。プロバイダ２は自分のコンテンツを秘密の鍵Ｋを用いて暗号化する。この暗号化については慣用鍵暗号でも公開鍵暗号でもよい。次にプロバイダ２はＥを用いてＫを、

【００２２】

【数１】$K' = K^E \mod n$

のように暗号化して、Ｋ’を得る。そして、暗号化したコンテンツとともに利用者３に配布する。ここで、Ｋ’は利用者３にはそれとわからない様にコンテンツ内に封入する。

【００２３】利用者３はチケットを取得するため、自分のＩＤとチケット法数ｎを管理センタ１に送る。管理センタ１は、利用者３のＩＤから検索した利用者３の秘密情報ｄｕと、チケット法数ｎとそれに対応するチケット公開鍵Ｅから生成した秘密情報Ｄを以下のように生成する。

【００２４】

【数２】

$$ED = 1 \mod \phi(n) \qquad (1)$$

ただしφ（ｎ）はｎのオイラー数で、ｐ、ｑから生成される。

【００２５】このＤを用いて、チケットｔを以下の様に生成し、利用者３に送る。

【００２６】

【数３】

$$t = D - F(du, L) + w\phi(n) \qquad (2)$$

ただし、ここで、ｗ＝Ｇ（ｄｕ，Ｌ）、Ｇ（）は適当な＊に基づいてΔを求める。次に求めたΔを用いて、新しい補助情報ｔｎｅｗを

$$tnew = told + \Delta$$

＊非衝突関数、Ｆは一方向性を持つ変換あるいは関数、Ｌは資源の利用条件等を記述した制御情報である。

【００２７】利用者３は発行されたｔを用いて、コンテンツに以下のようにアクセスする。まず、利用者３は、乱数ｒを生成し、以下のチャレンジＣを計算する。

【００２８】

【数４】

$$C = r^E \cdot K' \mod n \qquad (3)$$

以上の計算はコンテンツ利用プログラム３２内で行われる。

【００２９】コンテンツ利用プログラム３２はトークン３１と通信し、Ｃをトークン３１に送る。トークン３１内では、

【００３０】

【数５】

$$R = C^{t+F(du,L)} \mod n \qquad (4)$$

を計算しコンテンツ利用プログラム３２に戻す。

【００３１】利用者３側では、コンテンツ利用プログラム３２がＲを用いて、

【００３２】

【数６】

$$K = r^{-1} \cdot R \mod n \qquad (5)$$

によりＫを求め、コンテンツを復号化する。ここではじめて利用者はコンテンツの利用が可能となる。

【００３３】以上、本発明の実施例の前提とする技術について説明した。以下、本発明の実施例について説明する。なお、以下に示す実施例では、前述のチケットを補助情報、Ｌを制御情報と考え、本発明による証明データ生成手法を前述のトークン内に実装する。このような構成をとることで、利用者はＬをトークンに与えることで、新しいチケットｔを得ることができる。

［実施例１］図２に本発明による証明データ生成手法の一実施例を示す。図２において、１０１は制御情報、１０２は制御情報１０１に対応した補助情報、１０３が新規制御情報、１０４は制御情報、補助情報、および、新規制御情報１０３とから新規補助情報を生成する補助情報生成手段、１０５は新たに生成される補助情報である。

【００３４】この構成において、証明データ生成手段１０４は、与えられた制御情報１０１と新規制御情報１０３とを用いて、補助情報１０２を変更し、新規補助情報１０５として出力する。具体的には、すでに取得してある補助情報と制御情報をそれぞれ、ｔｏｌｄ，Ｌｏｌｄ、新しい制御情報Ｌｎｅｗとし、

【００３５】

【数７】

$$\Delta = F(du, Lold) - F(du, Lnew) \qquad (6)$$

※【００３６】

【数８】

※

$$tnew = told + \Delta \qquad (7)$$

のように生成する。

【００３７】図３に実施例１を実現する証明データ生成装置の構成例を示す。この図において、制御情報１０１、補助情報１０２、新規制御情報１０３、および、新規補助情報１０５は図２と同様である。２０１は証明データ生成装置、２０２は外部から制御情報１０１、および新規制御情報１０３を入力する制御情報入力部、２０３は外部から補助情報を入力する補助情報入力部、２０４は入力された補助情報および制御情報を転送するデータバス、２０５は変更された制御情報と補助情報から新たな補助情報生成する補助情報生成部、２０６は生成された新規補助情報１０６を出力する補助情報出力部である。

【００３８】この構成において、補助情報１０２を補助情報入力部２０３から入力するとともに、補助情報１０２に対応する制御情報１０１を制御情報入力部２０２に入力する。さらに利用者が新規の制御情報を制御情報入力部２０２に入力する。入力された制御情報および補助情報はデータバス２０４を通じて、補助情報生成部２０５に送られる。補助情報生成部２０５は送られてきた制御情報と補助情報から新規補助情報を、例えば前述の式（７）に基づいて計算し、結果をデータバス２０４を通じて、補助情報出力部２０６に送る。補助情報出力部２０６は送られてきた新規補助情報１０５を出力する。

【００３９】図４は図３の証明データ生成装置の変形例を示す。図４において、制御情報１０１、補助情報１０２、新規制御情報１０３、新規補助情報１０５、証明データ生成装置２０１、制御情報入力部２０２、補助情報入力部２０３、データバス２０４、補助情報生成部２０５、および、補助情報出力部２０６は図３と同様である。３０１は入力された制御情報を記憶する制御情報記憶部である。

【００４０】この構成において、入力された制御情報１０１はデータバス２０４を通じて制御情報記憶部３０１に送られ、保持される。次に新規の制御情報１０３が入力されると、記憶されている制御情報１０１を読み出して、データバス２０４を通じて補助情報生成部２０５に送る。この際、制御情報記憶部３０１内の制御情報１０３を新規制御情報１０５に置き換える。この場合置き換えず、記憶部内に新規制御情報を追加記憶するようにしても良い。このようにすることで、外部から入力される制御情報を用いず、記憶部内の制御情報のみを用いるようにすることもできる。さらに、コンテンツの利用と対応させることで利用履歴として取り扱い、例えば、利用状況に応じた課金や、さらに細かい制御情報の変更の制御を行う際に利用してもよい。

【００４１】図５は図３の証明データ生成装置の他の変形例を示す。図４において、制御情報１０１、補助情報１０２、新規制御情報１０３、新規補助情報１０５、証明データ生成装置２０１、制御情報入力部２０２、補助情報入力部２０３、データバス２０４、補助情報生成部２０５、補助情報出力部２０６、および制御情報記憶部３０１は図３と同様である。４０１は補助情報１０２の正当性を検査する検査部である。

【００４２】この構成において、まず、補助情報については、発行時に管理センタがセンタ自身の電子署名をセンタの秘密鍵で行う。検査部４０１内ではセンタの公開鍵を用いて署名の検証を行う。さらに発行時に補助情報または制御情報が、正当な利用者のみが使用できるように、利用者の公開鍵を用いて暗号化したものを発行し、利用者は利用者の秘密鍵で復号化する。これにより、補助情報１０２の正当性を検証できる。

【００４３】［実施例２］図６に本発明の証明データ生成手法の他の実施例を示す。図６において、制御情報１０１、補助情報１０２、新規制御情報１０３、補助情報生成手段１０４および、新規補助情報１０５は図１と同様である。５０１は制御情報生成手段である。

【００４４】この構成において、最初に与えられた制御情報１０１を、補助情報生成手段１０４に送るとともに、制御情報生成手段５０１に送る。制御情報生成手段５０１は入力された制御情報を適当な条件に照らして書き換え、新規制御情報１０３を生成する。

【００４５】図７に実施例２の証明データ生成手法を実現する証明データ生成装置の構成例を示す。図７において、制御情報１０１、補助情報１０２、新規制御情報１０３、新規補助情報１０５、証明データ生成装置２０１、補助情報入力部２０３、データバス２０４、補助情報生成部２０５、および、補助情報出力部２０６、制御情報記憶部３０１は図４と同様である。６０１は制御情報を変更して新規制御情報１０３を生成する制御情報生成部である。

【００４６】全体の動作は図４と共通である。したがって構成上異なる制御情報生成部６０１の動作について説明する。制御情報生成部６０１は、データバス２０４経由で制御情報記憶部３０１から制御情報１０１を読み出し、所定の条件に従い制御情報１０１を変更し新規制御情報１０３を生成する。

【００４７】図８に、図６における制御情報生成手段５０１（図７の制御情報生成部６０１）の動作を示す。図８において、制御情報１０１、新規制御情報１０３、制御情報生成部５０１は図６と同様である。７０１は制御情報の生成を制御する生成制御情報、７０２は生成の可否を決定する生成制御条件７０３は生成内容を規定する生成方法設定情報である。

【００４８】この構成において、制御情報１０１が、制御情報生成部５０１に入力されると、その時点の条件を生成制御情報７０１内の生成制御条件７０２と比較し、所定の条件を満たせば、生成制御情報７０１内にあり、生成制御条件７０２に対応する生成方法設定情報７０３にしたがって制御情報１０１を変更し、新規制御情報１

０３を生成し出力する。

【００４９】図９に、図８における生成制御条件７０２に、使用回数を用いた動作例を示す。図９において、使用回数がそれぞれｎ１、ｎ２、．．ｎｋ以下のとき生成方法設定情報７０３が設定１、設定２、．．設定ｋとなるようにしている。生成方法設定情報７０３として、例えば１回あたりの使用単価を用いて、使用回数がある程度増えると、割引価格で使用できるようにすることができる。あるいは、生成方法設定情報７０３として、使用権限を設定に用いて、ある回数を使用すると使用不可能になるようにしてもよい。

【００５０】図１０に、図８における生成制御条件７０２に、使用時間を用いた動作例を示す。図１０において、使用時間がそれぞれｔ１、ｔ２、．．ｔｋ以下の場合に生成方法設定情報７０３が設定１、設定２、．．設定ｋとなるようにしている。生成方法設定情報７０３として、例えば１回あたりの使用単価を用いて、使用時間がある程度増えると、割引価格で使用できるようにすることができる。あるいは、生成方法設定情報７０３として、使用権限を設定に用いて、ある期間使用すると使用不可能になるようにしてもよい。

【００５１】図１１に図７の制御情報生成部６０１の構成を示す。図１１において、制御情報１０１、新規制御情報１０３、制御情報生成部、データバス２０４は図７と同様である。１００１は、データバス２０４経由で制御情報と生成制御情報１００３の入出力を行う入出力部、１００２は、生成制御情報１００３に基づいて、新規制御情報１０３を生成する生成部、１００３は、新規制御情報の生成方法を規定する生成制御情報、１００４は、内部データバスである。

【００５２】この構成において、データバス２０４から、制御情報１０１、および、生成制御情報１００３を、入出力部１００１が読み込む。読み込んだ結果を生成部１００２に送ると、生成部１００２は生成制御情報を解読し、その結果に基づいて、制御情報１０１から新規制御情報１０３を生成する。新規制御情報１０３は、入出力部１００１からデータバス２０４に出力される。

【００５３】図１２に図７の制御情報生成部６０１の構成を示す。図１２において、制御情報１０１、新規制御情報１０３、制御情報生成部、データバス２０４入出力部１００１、生成部１００２、生成制御情報１００３、内部データバス１００４は図１１と同様である。１１０１は、生成制御情報を記憶する生成制御情報記憶部である。

【００５４】この構成において、新規制御情報１０３の生成方法は、図１１と同様であるが、使用する生成制御＊情報１００３を、生成情報記憶部１１０１から内部データバス１００４経由で読み出して用いる。生成制御情報記憶部１１０１内部の生成制御情報１００３は、データバス２０４、入出力部１００１経由で外部から読み込んでも、例えばＲＯＭチップのような半導体に半永久的に書き込んだ形式で提供してもよい。

【００５５】以上で実施例の説明を終了する。なお、本発明は上述の実施例に限定されるものではなく種々の変更が可能である。例えば、上述の実施例では補助情報を利用者の固有情報と制御情報とに基づくものとしたが、補助情報を制御情報のみに基づくものとしてもよい。

【００５６】

【発明の効果】以上説明したように、本発明によれば、使用者側において、制御情報に基づいて補助情報が変更されるので、制御情報が変更される度にセンタ側から利用者に補助情報を送る必要がなくなる。

【図面の簡単な説明】

【図１】　本発明の実施例が適用される認証システムを説明する図である。

【図２】　本発明の実施例１の証明データ生成手法を説明する図である。

【図３】　実施例１を実現する証明データ生成装置の構成例を示すブロック図である。

【図４】　実施例１の証明データ生成装置の他の構成例を示すブロック図である。

【図５】　実施例１の証明データ生成装置の他の構成例を示すブロック図である。

【図６】　本発明の実施例２の証明データ生成手法を説明する図である。

【図７】　実施例２を実現する証明データ生成装置の構成例を示すブロック図である。

【図８】　実施例２の要部を説明する図である。

【図９】　実施例２の要部の動作を説明する図である。

【図１０】　実施例２の要部の動作を説明する図である。

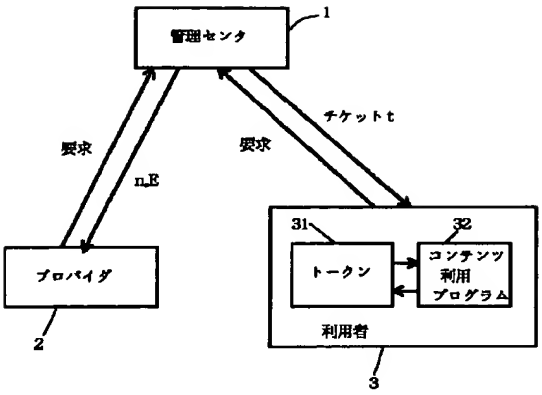
【図１１】　図７の証明データ生成装置の制御情報生成部の構成例を示すブロック図である。

【図１２】　図７の証明データ生成装置の制御情報生成部の他の構成例を示すブロック図である。

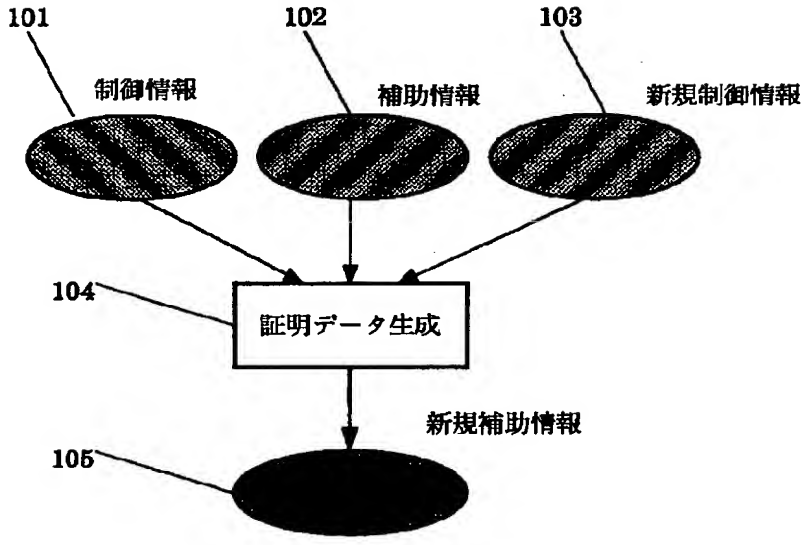
【符号の説明】

２０１　証明データ生成装置
２０２　制御情報入力部
２０３　補助情報入力部
２０５　補助情報生成部
２０６　補助情報出力部

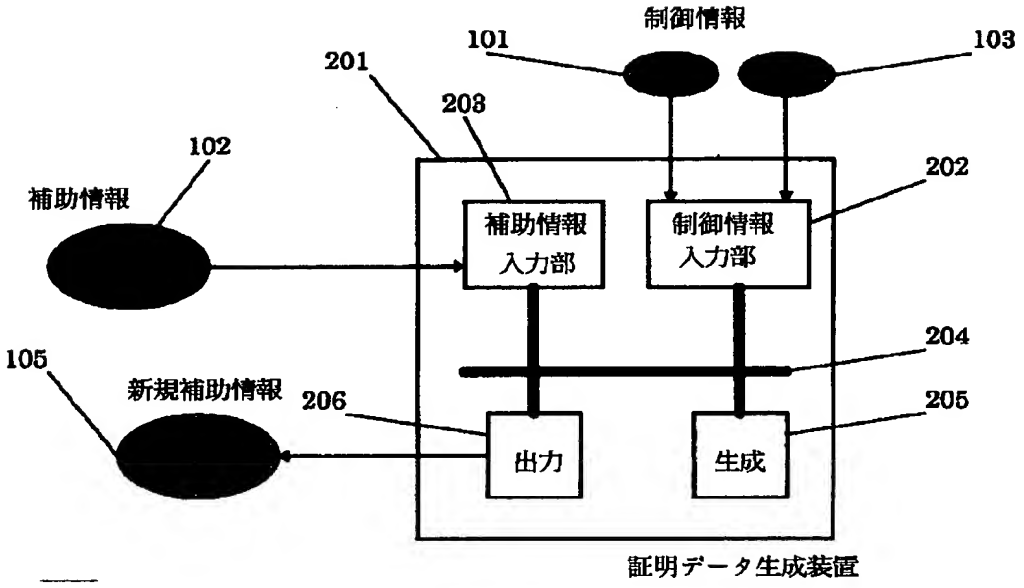
【図１】


管理センタ
1
要求
n,E
要求
チケットt
プロバイダ
2
31
32
トークン
コンテンツ利用プログラム
利用者
3

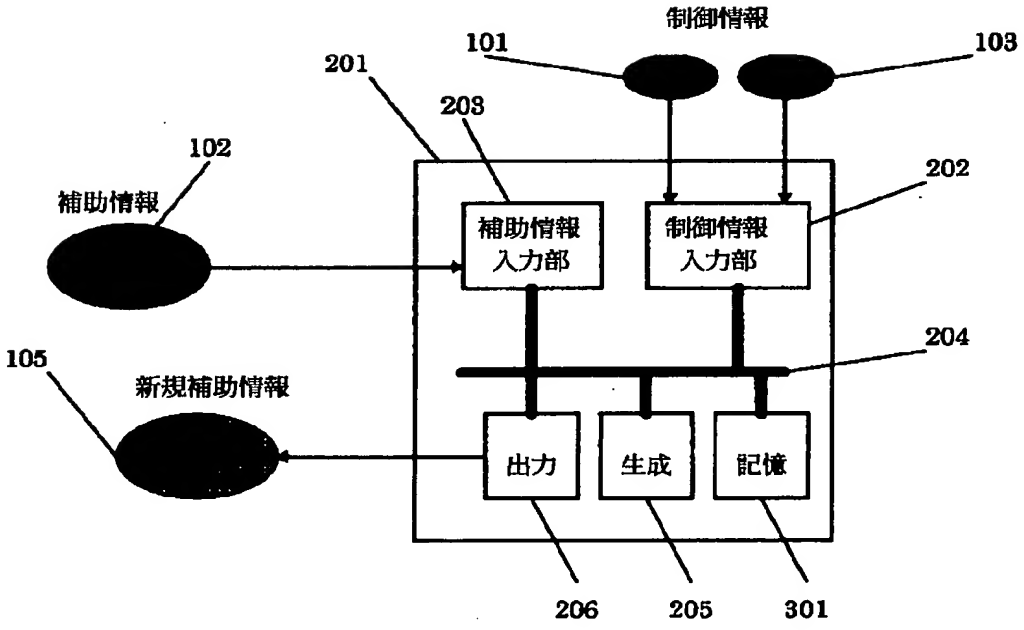
【図２】


101
制御情報
102
補助情報
103
新規制御情報
104
証明データ生成
新規補助情報
105

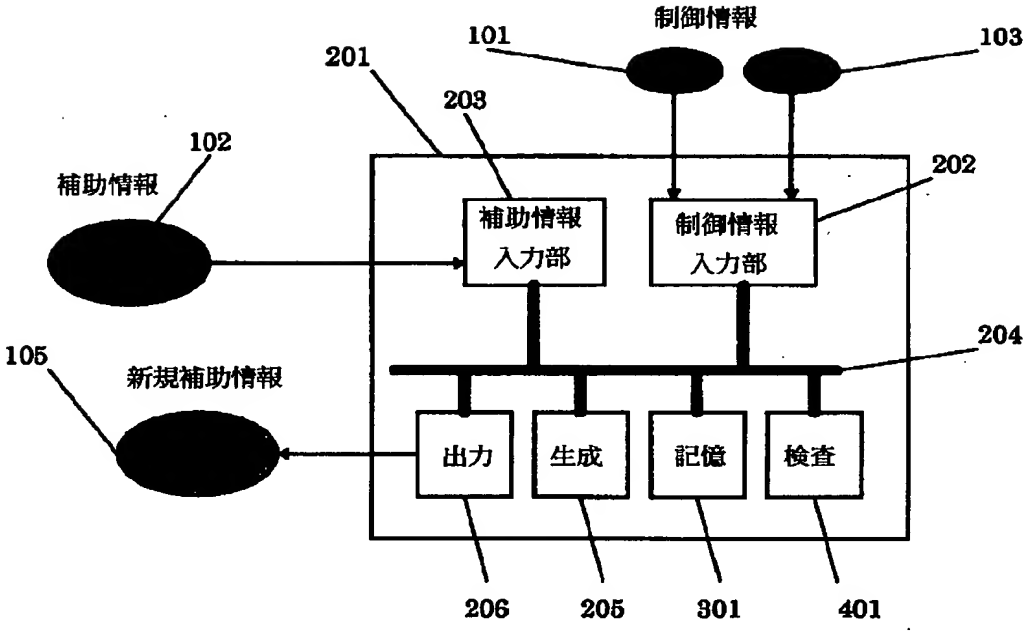
【図３】


制御情報
101
103
201
208
102
補助情報
202
補助情報
入力部
制御情報
入力部
204
105
新規補助情報
206
205
出力
生成
証明データ生成装置

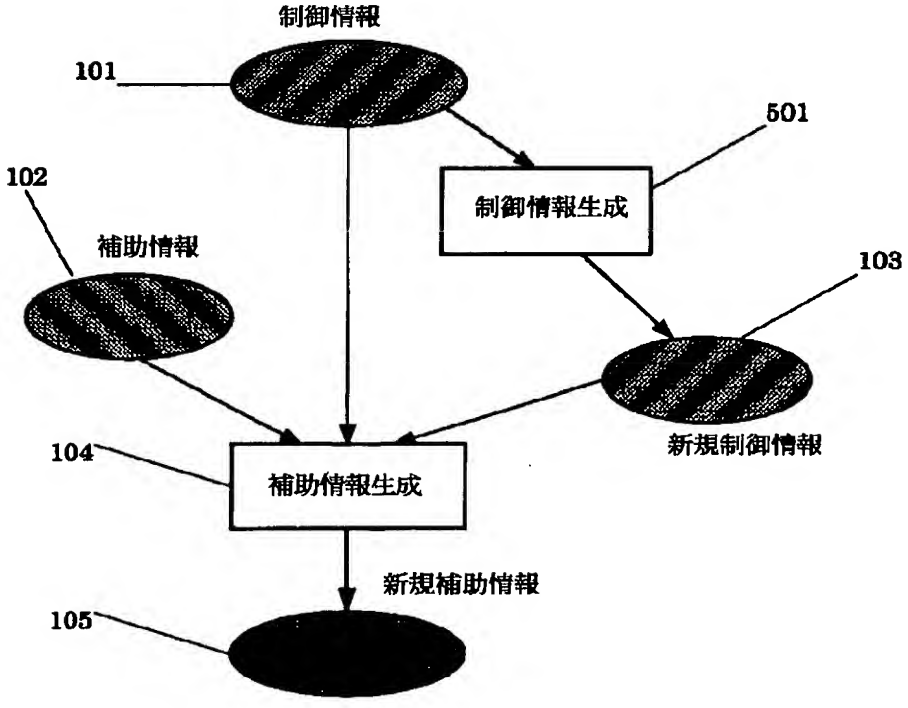
【図４】


制御情報
101
103
201
203
102
補助情報
202
補助情報
入力部
制御情報
入力部
204
105
新規補助情報
出力
生成
記憶
206
205
301

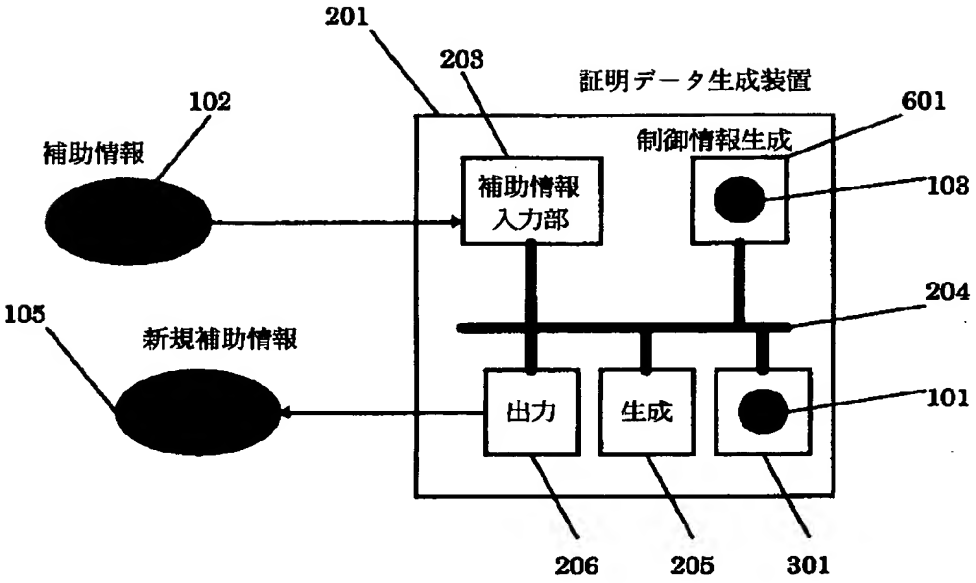
【図５】


制御情報
101
103
201
203
102
補助情報
202
補助情報
入力部
制御情報
入力部
204
105
新規補助情報
出力
生成
記憶
検査
206
205
301
401

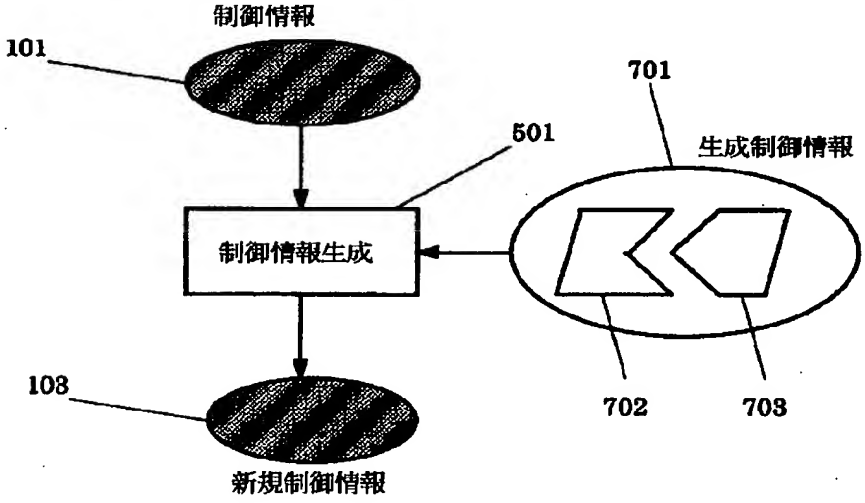
【図６】


制御情報
101
501
102
制御情報生成
補助情報
103
新規制御情報
104
補助情報生成
新規補助情報
105

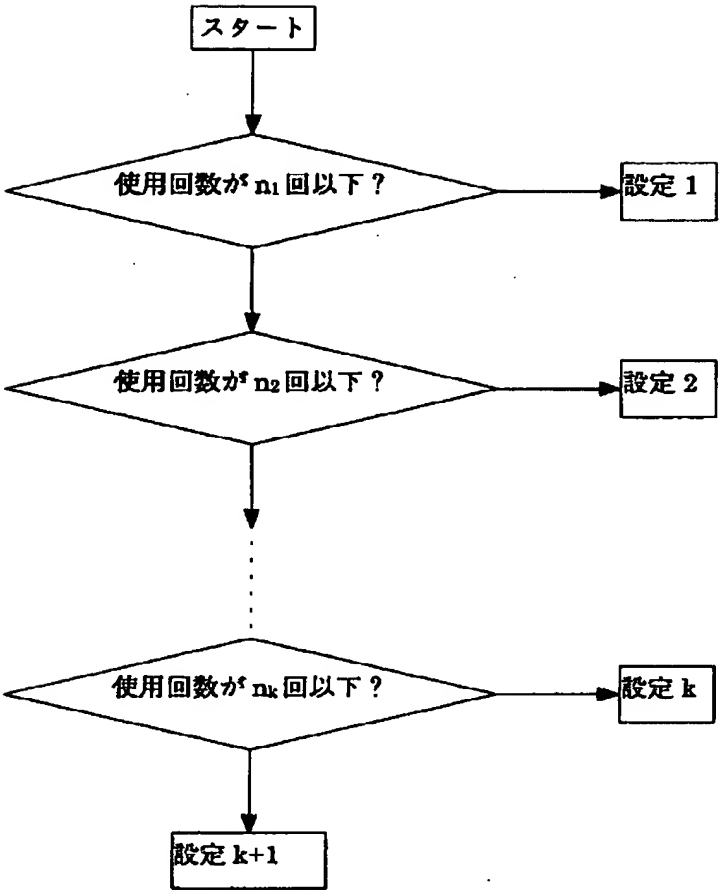
【図７】


201
208
証明データ生成装置
102
補助情報
601
制御情報生成
補助情報
入力部
103
204
105
新規補助情報
出力
生成
101
206
205
301

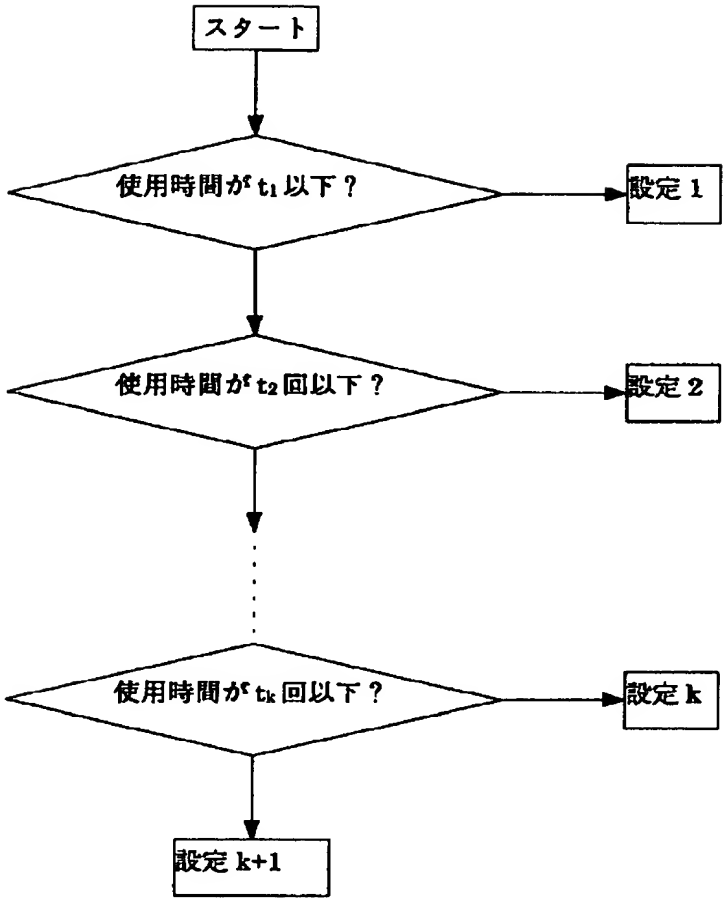
【図８】


制御情報
101
701
501
生成制御情報
制御情報生成
108
702
703
新規制御情報

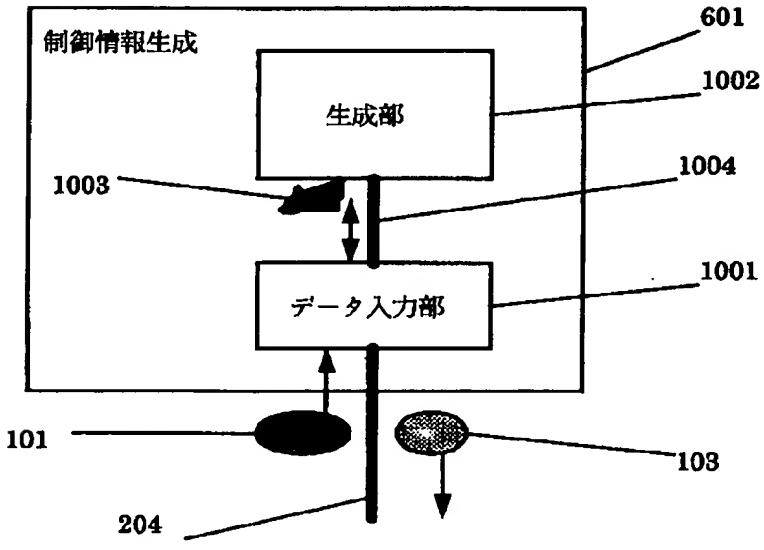
【図９】



【図１０】


スタート
使用時間が t1 以下？
設定 1
使用時間が t2 回以下？
設定 2
使用時間が tk 回以下？
設定 k
設定 k+1

【図１１】


制御情報生成
601
生成部
1002
1003
1004
データ入力部
1001
101
103
204

【図１２】